



Cyber Legal Awareness Program for Youngsters

Dr. Jim Q. Chen, DoD National Defense University

Ms. Mary Lin, DoD Defense Information Systems Agency

Mr. Pedro D. Cordero, FBI Supervisory Special Agent (SSA)

Agenda

- Current issues and challenges
- Solution rooted in education
- Curriculum for cyber legal awareness program

Current Situation

- Hacking in cyberspace: not that difficult with tools
- Examples of penalties:
 - Penalties for hacking: Class B misdemeanor, 6 months in prison, up to \$1,000 fine, or both
 - Penalties for child pornography: 18 USC 2251, fines + a statutory 15-30 years in prison
- No cyber crime education for youngsters, parents, and the general public

Different Types of Actors

- Nation-state
- Criminal groups
- Hacktivists
- Individuals who wants to show off
- Individuals who are interested in exploration
- Individuals who accidentally get trapped into it

How to Reduce Cyber Crime

- Cyber defense
- Law enforcement
- Education and awareness training

Cyber Crime Prevention

- Social aspect
- Technical aspect
- Legal aspect
- Etc.

Social Aspect

- Young people: a lot of time spent on the Internet
- Loneliness
- Busy parents
- Attractive computer/Internet games
- Lack of role models
- Unsafe virtual environment

Technical Aspect

- Proliferation of technologies, especially smart devices
- Easy access to hacking tools
- Integration into the physical world: Cyber-physical, IoTs

Legal Aspect

- Internet contents: not regulated
- Legal burden: on consumers
- Cyber law: behind technology

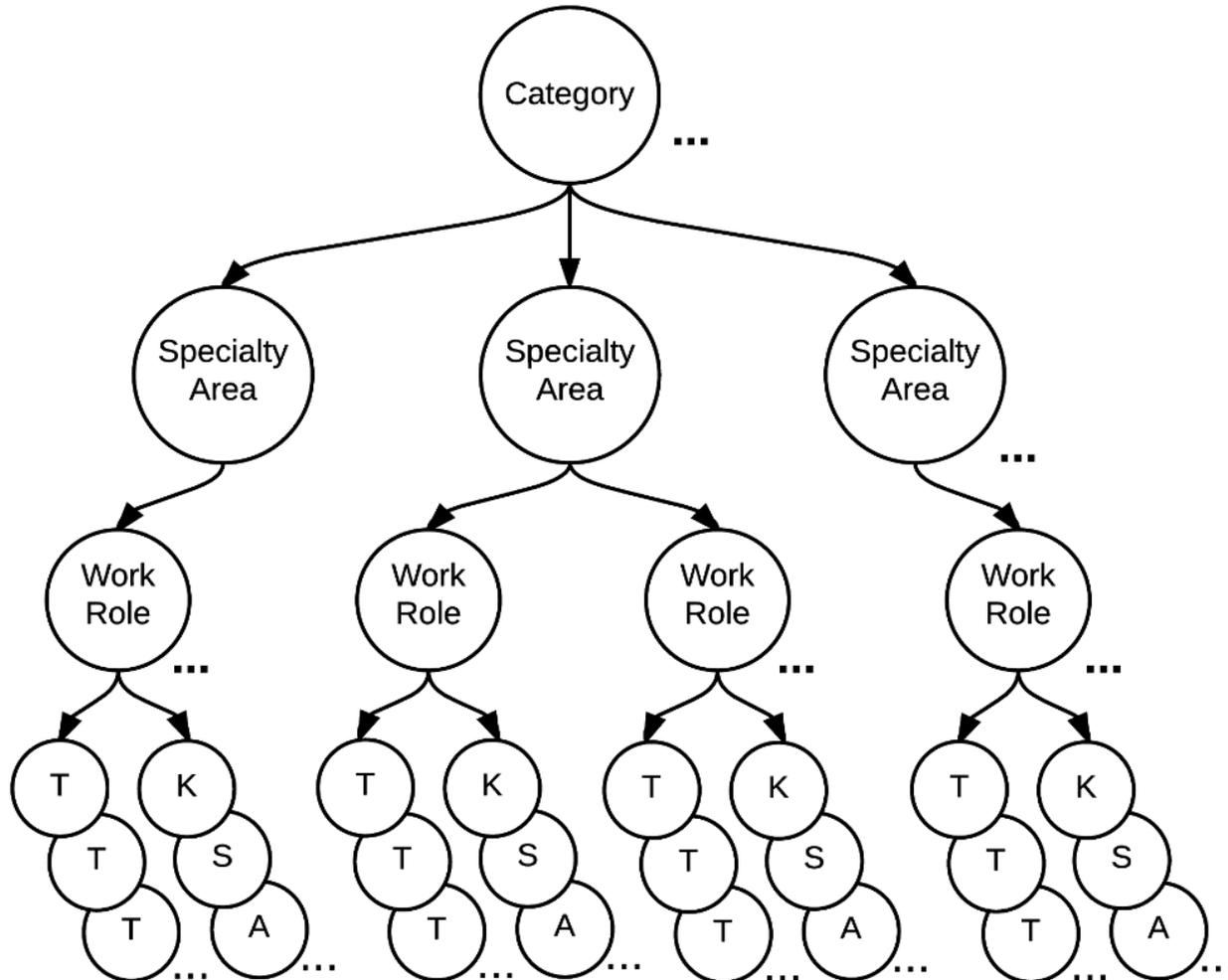
What Is Missing?

- Lack of cyber crime education
- Lack of mental health education and treatment
- Lack of depression prevention program
- Lack of cyber crime prevention program

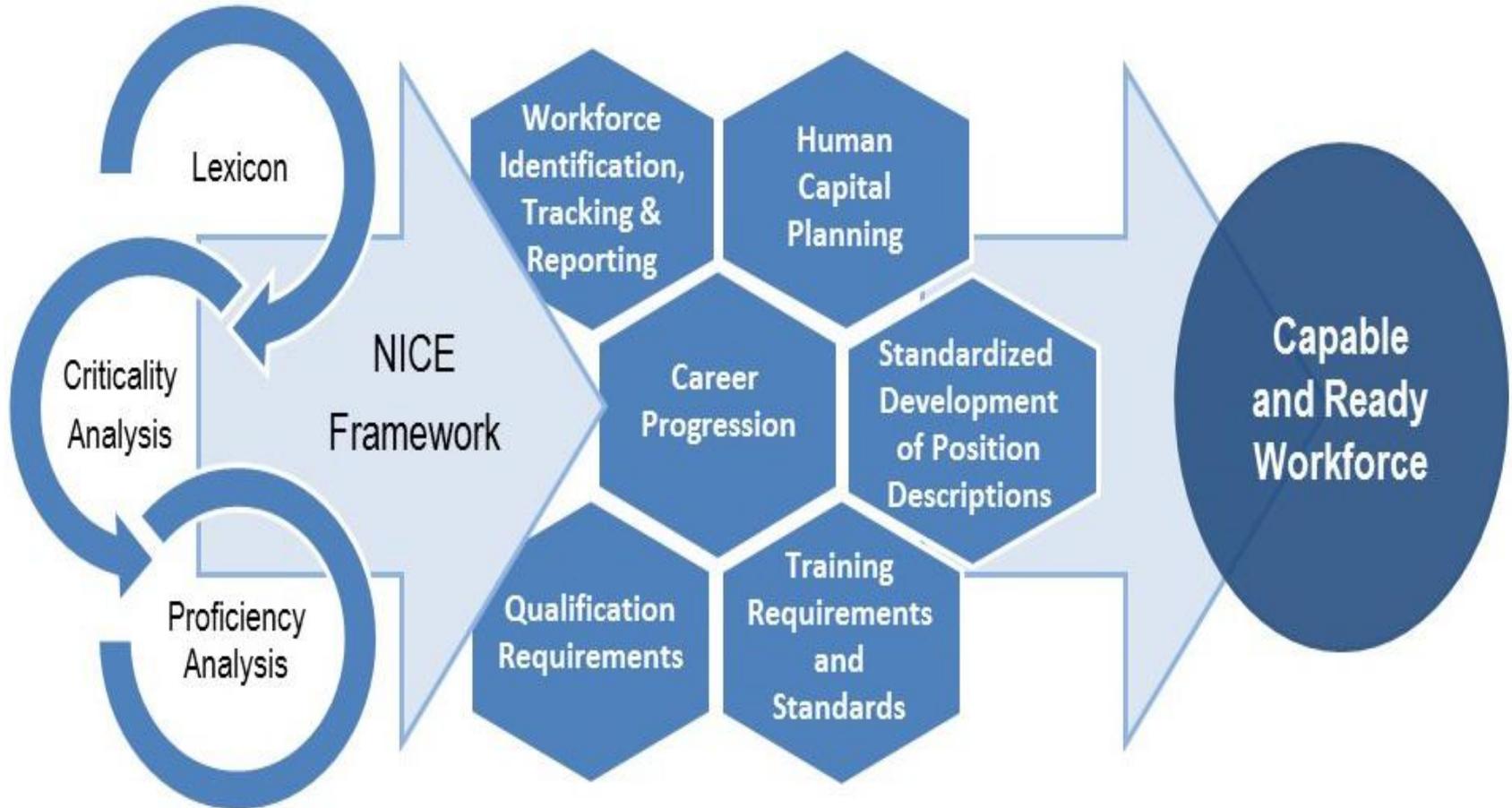
Solution

- Establish a cyber crime awareness program
- Questions:
 - What should be taught in this program?
 - What should the curriculum of such a program look like?
 - How should this program be taught?

NICE Framework Components



Building Blocks



Cyber Legal Advisor

- **Work Role Name:** Cyber Legal Advisor
- **Work Role ID:** OV-LGA-001
- **Specialty Area:** Legal Advice and Advocacy (LGA)
- **Category :** Oversee and Govern (OV)
- **Work Role Description:** Provides legal advice and recommendations on relevant topics related to cyber law.
- **Tasks:**
 - T0006, T0098, T0102, T0131, T0220, T0419, T0434, T0465, T0474, T0476, T0478, T0487, T0522
- **Knowledge:**
 - K0001, K0002, K0003, K0004, K0005, K0006, K0017, K0059, K0107, K0157, K0261, K0262, K0267, K0312, K0316, K0341, K0615
- **Skills:**
 - S0356
- **Abilities:**
 - A0046

Categoryzation

- 1) Knowledge: cyberspace and Cyber law
- 2) Application of law
- 3) Organizational legal affairs

Cyber Instructor

- **Work Role Name:** Cyber Instructor
- **Work Role ID:** OV-TEA-002
- **Specialty Area:** Training, Education, and Awareness (TEA)
- **Category :** Oversee and Govern (OV)
- **Work Role Description:** Develops and conducts training or education of personnel within cyber domain.
- **Tasks:**
 - T0030, T0073, T0101, T0224, T0230, T0247, T0316, T0317, T0318, T0319, T0320, T0321, T0322, T0323, T0352, T0365, T0367, T0381, T0382, T0395, T0443, T0444, T0450, T0451, T0467, T0519, T0520, T0535, T0536, T0926
- **Knowledge:**
 - K0001, K0002, K0003, K0004, K0005, K0006, K0007, K0059, K0115, K0124, K0130, K0146, K0147, K0204, K0208, K0213, K0215, K0216, K0217, K0218, K0220, K0226, K0239, K0245, K0246, K0250, K0252, K0287, K0313, K0319, K0628
- **Skills:**
 - S0001, S0004, S0006, S0051, S0052, S0053, S0055, S0056, S0057, S0060, S0064, S0070, S0073, S0075, S0076, S0081, S0084, S0097, S0098, S0100, S0101, S0121, S0131, S0156, S0184, S0270, S0271, S0281, S0293, S0301, S0356, S0358

Cyber Instructor

- **Abilities:**

- A0006, A0011, A0012, A0013, A0014, A0015, A0016, A0017, A0018, A0019, A0020, A0022, A0023, A0024, A0032, A0055, A0057, A0057, A0058, A0063, A0066, A0070, A0083, A0089, A0105, A0106, A0112, A0114, A0118, A0119, A0171

Categorization

- 1) Knowledge: cyberspace and General
- 2) Analytical Thinking
- 3) Knowledge: Cyber Law
- 4) Communications/Writing
- 5) Teaching

OV-LGA-001 vs. OV-TEA-002

<u>OV-LGA-001</u>	<u>OV-TEA-002</u>
<u>Knowledge: Cyberspace & Cyber Law</u>	<u>Knowledge: Cyberspace & General</u>
	<u>Analytical Thinking</u>
	<u>Knowledge: Cyber Law</u>
	<u>Communications</u>
	Teaching
Application of Law	
Organizational Legal Affairs	

Curriculum

- Cyberspace Fundamentals
- Analytical Thinking
- Cyber Law
- Communications

Conclusion

- Cyber Crime Awareness Education is badly needed.
- NIST NICE Framework provides a good and practical guidance in developing a curriculum.
- Varied methods should be utilized to implement the curriculum.

Questions?

